IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA

v.

MICHAEL CHARLES SCHENA,

Defendant.

No. 1:25-CR-158

STATEMENT OF FACTS

The United States and the defendant, Michael Charles Schena (hereinafter, "the defendant"), agree that at trial, the United States would have proven the following facts beyond a reasonable doubt:

1. From in or about 2023 through in or around February 2025, in the Eastern District of Virginia and elsewhere, including outside of the jurisdiction of any particular State or district of the United States, within the extraterritorial jurisdiction of the United States, the defendant, having possession of, access to, and control over information and documents relating to the national defense, conspired with others to willfully transmit SECRET information and documents to persons not entitled to receive them, with reason to believe that the information so transmitted could be used to the injury of the United States or to the advantage of a foreign nation.

The Defendant's Department of State Employment and Access to Classified Information

2. The defendant is employed by the United States Department of State ("DOS") as a South Caribbean Desk Officer in the Bureau of Western Hemisphere America, located at DOS Headquarters in Washington, DC. During the relevant time period, the defendant held a TOP SECRET security clearance.

3. Pursuant to Executive Order 12958 signed on April 17, 1995, as amended by Executive Order 13292 on March 25, 2003, and Executive Order 13526 on December 29, 2009, national security information was classified as "TOP SECRET," "SECRET," or "CONFIDENTIAL." National security information was information owned by, produced by, produced for, and under the control of the United States government that was classified as follows:

a. Information was classified as TOP SECRET if the unauthorized disclosure of that information reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority was able to identify and describe.

b. Information was classified as SECRET if the unauthorized disclosure of that information reasonably could be expected to cause serious damage to the national security that the original classification authority was able to identify and describe.

c. Information was classified as CONFIDENTIAL if the unauthorized disclosure of that information reasonably could be expected to cause damage to the national security that the original classification authority was able to identify and describe.

4. Information classified at any level could only be lawfully accessed by persons determined by an appropriate United States government official to be eligible for access to classified information, who received a security clearance, who had signed an approved non-disclosure agreement, and who had a "need to know" the classified information. Classified information could only be stored in an approved facility or container, or on an approved computer network.

5. Through his employment, the United States Government entrusted the defendant with access to sensitive government materials, including information relating to the national defense that was closely held by the government ("National Defense Information") and classified documents and materials.

6. On January 9, 2006, the defendant signed a Classified Information Nondisclosure Agreement acknowledging, among other things, that he received a security indoctrination

concerning the nature and protection of classified information. Further, in that agreement the defendant agreed that he had been advised that any breach may, among other penalties, constitute violations of United States criminal laws.

7. The defendant had access to materials classified up to the SECRET level while in his physical workspace at DOS located in Washington, D.C. However, the defendant also conducted work from his home in Alexandria, Virginia, where he had access to information classified up to the Sensitive But Unclassified (SBU) level from his DOS issued laptop computer.

The Defendant's Conspiracy to Unlawfully Transmit Classified Information and Documents

8. Beginning at least in or about April 2022, the defendant communicated with people he met online through various communication platforms and provided to them information to which they were not entitled. These individuals paid the defendant for the provision of this information.

9. For example, on or about April 11, 2022, the defendant received a message on a social media platform from a user on the platform (Platform User 1) who stated they worked for an international consulting company and inquired about the defendant's interest in working with them. The defendant replied indicating his interest. Over the following weeks, the defendant and Platform User 1 attempted to schedule video teleconference calls and identify a successful method for Platform User 1 to pay the defendant. On or about May 18, 2022, Platform User 1 attempted to pay the defendant $500 in $100 increments, but the transactions failed. Shortly thereafter, a successful payment was made for $500. Approximately six hours after that payment was made, Platform User 1 asked the defendant to resend the "pictures" with a higher quality resolution. The $500 payment was compensation for photographed documents, notes, files, or other information of interest to the PRC.

10. On or about June 19, 2022, the defendant emailed Platform User 1 the text from a State Department document, which had SBU markings. However, the defendant removed some, but not all, SBU markings from the document prior to sending it to Platform User 1. Approximately two days later, on June 21, 2022, the defendant received an online payment of $500.

11. Two additional individuals the defendant met online and provided information to in exchange for money are Unindicted Co-Conspirator 1 ("UCC 1") and Unindicted Co-Conspirator 2 ("UCC 2"). The defendant believed UCC 1 and UCC 2 worked for a foreign government, specifically the People's Republic of China.

12. In and around August 2024, at UCC 1's direction, the defendant met an unknown individual at a hotel in Peru. This individual gave the defendant $10,000 in United States currency and a white Apple iPhone 14. This white Apple iPhone 14, which is registered with a foreign telephone number, was intended as a covert communication device for the defendant to image and/or transmit information without law enforcement detection to UCC 1 and possibly others who are not otherwise authorized to receive this information. The defendant also communicated with UCC 1 and UCC 2 on this white Apple iPhone 14 and received taskings from UCC 1 and UCC 2. The defendant did not receive approval by anyone at DOS to image, store, or disseminate classified material on the white Apple iPhone 14.

13. On October 25, 2024, the defendant accessed the DOS classified system and saved five SECRET level reports to a folder on his classified system's desktop. On October 29, 2024, the defendant attempted to print some of these SECRET level reports but was unable to map the printer in his office. The defendant then photographed the reports using the white Apple iPhone 14 he obtained in Peru. The defendant then sent four of the five reports to UCC 1 later that

evening. These documents contained national defense information. The documents were all visibly marked with SECRET classification markings.

14. On February 17, 2025, the defendant accessed the DOS system from Alexandria, Virginia, within the Eastern District of Virginia, and downloaded a document visibly marked as SBU. The defendant then attempted to email the document from his DOS email account to his personal email account. However, after receiving an alert that emailing the sensitive but unclassified information may violate DOS policy, the defendant classified his email as Unclassified. The defendant then sent the email to his personal email account. The defendant then deleted the downloaded SBU document from his work issued computer and logged off.

15. On February 27, 2025, the defendant logged into the DOS classified enclave CLASSNET at his computer workstation in his DOS workspace. The defendant accessed at least five documents relating to the diplomatic relationship of the U.S. These documents contained national defense information. The documents were all visibly marked with SECRET classification markings. The defendant photographed the documents, which were displayed on his computer screen, with the white Apple iPhone 14 he received through UCC 1 in Peru.

16. The defendant then opened an application on the white Apple iPhone 14, typed a message in an application, and then inserted the photographs into the message. The defendant then deleted the photographs from the camera roll of the cell phone but did not completely delete the photographs off of the cell phone. The defendant then used his personal black Apple iPhone 14 to message UCC 1, "Send a link tonight" and to message UCC 2, "Have stuff tonight[.]" Shortly thereafter, the defendant left DOS and proceeded towards his home with both his white Apple iPhone 14 and black Apple iPhone 14. The defendant intended to send the classified documents he photographed to UCC 1 and UCC 2 that evening in the Eastern District of Virginia. However,

after leaving work on February 27, 2025, FBI special agents stopped the defendant outside of his residence in Alexandria, Virginia, and he was still in possession of the white iPhone 14, which agents seized at that time.

17. The white iPhone 14 contained four classified documents the defendant photographed on October 29, 2024 and seven classified documents the defendant photographed earlier on February 27, 2025. These documents related to the national defense of the United States. The defendant was not authorized to photograph any of these SECRET documents with the white Apple iPhone 14, was not authorized to retain these images on his Apple iPhone 14, and was not authorized to disseminate it to UCC 1, UCC 2, or others he met online.

*****

18. This statement of facts includes those facts necessary to support the plea agreement between the defendant and the United States. It does not include each and every fact known to the defendant or to the United States, and it is not intended to be a full enumeration of all of the facts surrounding the defendant's case.

19. The actions of the defendant, as recounted above, were in all respects knowing and deliberate, and were not committed by mistake, accident, or other innocent reason.

Respectfully submitted,

Erik S. Siebert
United States Attorney

Date: June 3, 2025

By: _____
Michael P. Ben'Ary
Gavin Tisdale
Assistant United States Attorney, EDVA

By: _____
Maria Fedor
Trial Attorney, CES

After consulting with my attorney and pursuant to the plea agreement entered into this day between the defendant, Michael Charles Schena, and the United States, I hereby stipulate that the above Statement of Facts is true and accurate, and that had the matter proceeded to trial, the United States would have proved the same beyond a reasonable doubt.

Michael Charles Schena

I am counsel for Michael Charles Schena and have carefully reviewed the above Statement of Facts with him. To my knowledge, his decision to stipulate to these facts is an informed and voluntary one.

Cadence Mertz
Counsel for Michael Charles Schena